

## 19:01 Let's start a band together!

Neighbors, please join me in reading this twentieth release of the International Journal of Proof of Concept or Get the Fuck Out, a friendly little collection of articles for ladies and gentlemen of distinguished ability and taste in the field of reverse engineering and the study of weird machines. This release is a gift to our fine neighbors in Heidelberg, Canberra and Knoxville.

If you are missing the first nineteen issues, we suggest asking a neighbor who picked up a copy of the first in Vegas, the second in São Paulo, the third in Hamburg, the fourth in Heidelberg, the fifth in Montréal, the sixth in Las Vegas, the seventh from his parents' inkjet printer during the Thanksgiving holiday, the eighth in Heidelberg, the ninth in Montréal, the tenth in Novi Sad or Stockholm, the eleventh in Washington D.C., the twelfth in Heidelberg, the thirteenth in Montréal, the fourteenth in São Paulo, San Diego, or Budapest, the fifteenth in Canberra, Heidelberg, or Miami, the sixteenth release in Montréal, New York, or Las Vegas, the seventeenth release in São Paulo or Budapest, the eighteenth release in Leipzig or Washington, D.C., or the nineteenth in Montréal. Two collected volumes are available through No Starch Press, wherever fine books are sold.

On page 5, our editor in chief regales us with tales of coke! Neither the soft drink nor the alkaloid, he speaks here of the refined coal that ushered in the Industrial Revolution, the compromises necessary to build an affordable bridge from wrought and cast iron when steel has yet to be invented, and the disastrous collapse of the Tay Bridge in Scotland. What modern marvels are made affordable and efficient by similar fancy tricks, only to collapse under an adversarial load?

Time and again in this journal, we have seen that regular expressions have been used in fragile code that rules our lives. On page 11, Jeff Dileo presents a trick for formatting Powershell scripts as email addresses, such that they are executed when exported by spammers into Microsoft Excel as CSV textfiles.

Every enterprising young lady and gentleman who has delved into datasheets and instruction sets has a moment of curiosity when a field is marked as undefined, or when it is defined to a constant with no explanation of that constant's meaning. Eric Davison shows on page 17 that, at least in the instruc-

tions of modern ARM executables, it is possible to scramble the constants, breaking compatibility with disassemblers while executing exactly as intended on real hardware. Perhaps you, dear reader, can do the same to other architectures?

After our paper release, and only when quality control has been passed, we will make an electronic release named `pocorgtfo19.pdf`. It is a valid PDF document, an HTML page, and a ZIP file filled with fancy papers and source code. You might also find `pocorgtfo19.exe`, `pocorgtfo19.png` and `pocorgtfo19.mp4` with the same MD5 hash. On page 21, our very own Ange Albertini will show you show he made this pileup of a polyglot and hash collisions.

There's a lot of fancy work that can be do with homoglyphs in UTF8, but what other clever things can be done with it? Ryan Speers and Travis Goodspeed have been fuzzing UTF8 interpreters not for crashes, but for differences of opinion on string legality. On page 39, they will show you how to make a string that is happily allowed by Java and Golang, but impossible to insert into a PostgreSQL table.



GRAPHTRIX™ 1.3

NEED  
HARD COPY OF YOUR APPLE II  
HI-RES GRAPHIC?  
WITH  
GRAPHTRIX™ 1.3  
YOU CAN  
INSERT YOUR  
GRAPHIC  
ANYWHERE  
IN YOUR  
TEXT.  
USE ANY OF  
19 PRINTERS  
AND  
10 INTERFACE CARDS.

From Data Transforms Inc.  
616 Washington, Suite 106  
Denver, Colorado 80203  
(303) 832-1501

Features: Graphic Magnification,  
Normal/Inverse, Page Centering,  
High and Low Crop Marks, Title String,  
Superscript, Footnotes, Chapters, Fully  
Menu Driven

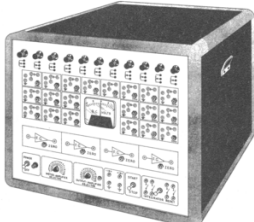
REQUIRES: Apple II with 48K, Applesoft  
in ROM, One Disk Drive with DOS 3.3.

Apple is a trademark of Apple Computer Inc.  
Copyright 1982 Data Transforms Inc. All Rights Reserved.  
GRAPHTRIX is the trademark of Data Transforms Inc., a division of Solaristics Inc.

**VERSATILE, LOW COST ANALOG COMPUTER**

**MODEL MK-1**

- LOW COST.
- FULLY TRANSISTORIZED.
- DESK TOP SIZE.
- FRONT PANEL ACCESS TO ALL ACTIVE COMPUTING ELEMENTS.
- AMPLIFIER OVERLOAD ALARM.
- PLUG IN MODULE ASSEMBLY.



**SPECIFICATIONS:**

- 20 operational amplifiers  $\pm 10$  volt output.
- 3  $\frac{X^2}{10}$  function generators.
- 1 5 log 10x function generator.
- 10 Potentiometers
- D.C. - 1 KC response.
- $\pm 5\%$  accuracy.
- 115 VAC supply required.

**BASIC EQUIPMENT:**

- MK-1 computer, cabinet mounted.
- 10 patch cords.
- 10 input-output feedback resistor jumpers (resistor values optional).
- 2 input-output feedback capacitor jumpers (capacitor values optional).

**INPUT:**

Tape recorder, transducers, or any external signal.

**OUTPUT:**

- Front panel meter.
- Scope
- Strip chart recorder.

**ACCESSORIES AVAILABLE:**

- Strip chart recorder.
- $X^2$ , log, and variable function generators.
- Patch cords and jumpers.

PRICE (with basic equipment) \$1,980<sup>00</sup>  
DELIVERY - 45 days

**CONTROL & COMPUTING DEVICES CO.**  
Box 925, Garland, Texas Phone RI-1-5443 (Dallas)

Even the best among us, having hoarded electronic components for years, sometimes lack that one nifty piece that would make a project work. Page 44 presents one such project, a vacuum fluorescent display driver that was saved by clever thinking and a refusal to give into frustration.

Rodger Allen presents us, on page 47, with a clever tool in Haskell that hides text in the unused space of .bmp and .ico palettes. You just might find a copy of its source code in the favicon of your favorite PoC||GTFO mirror!

We relax for intermission on page 53 with a delightful ditty by Dr. EVM and MMX Show, their hit single, The Pages of PoC||GTFO!

So there's this idea that wherever two users share a constrained resource, they can use it as a communications channel, just by hogging the resource or leaving it be. The faster and more tightly constrained the resource is, the better to communicate with it. On page 55, Lorenzo Benelli shows us that *vector multiplication* on Intel's AVX instruction set is a constrained resource, and that its startup and

shut down delays can be used as a communications channel. Isn't that wild?

Gabriel Radanne presents his Camelus Documentation on page 60, a PDF file that is also executable OCaml bytecode. The Sapir-Albertini hypothesis, you heard of it here first, neighbors!

You might remember Alexei Bulazel from his hilarious AVLeak research at WOOT, in which he exfiltrated file and registry listings from cloud antivirus products through thousands of preselected false positives and a fresh unpacker.<sup>1</sup> Windows Defender has been a pet research project of his, and on page 64, he explains the internals of its emulator. You'll learn how its custom `apicall` instruction can be added to IDA Pro, how to add an output channel for `printf()` debugging from the emulator, and how to bypass Microsoft's mitigations against abuse of this emulation layer.

On page 80, the last page, we pass around the collection plate. Our church has no interest in bitcoins or wooden nickels, but we'd love your donation of a reverse engineering story. Please send one our way.

BINARY VISION

GRAPHIC ARTIST

Excellent freelance artist with 16-bit experience needed to work on interactive CD projects. Good rates and interesting work.

Please send ST/Amiga demo discs to Rupert Bowater, BINARY VISION, 447 Green Lanes, Haringey N4 1HA or phone (4-7pm) : 081 341 6866

<sup>1</sup>unzip pocorgtfo19.pdf avleak.pdf